Survivability for Public Safety Networks

Dr. Vanu G. Bose
CEO
Vanu, Inc.

Reliability
≠
Survivability

- **Yet commercial wireless network metrics and standards are being used to drive the design of the FirstNet Nationwide Public Safety Network.**
- **This approach will result in a significantly more costly network that will still fail in the face of disaster scenarios.**
- **The work presented here sets the ground work for developing alternative metrics and design principles for networks where survivability is the most important goal.**

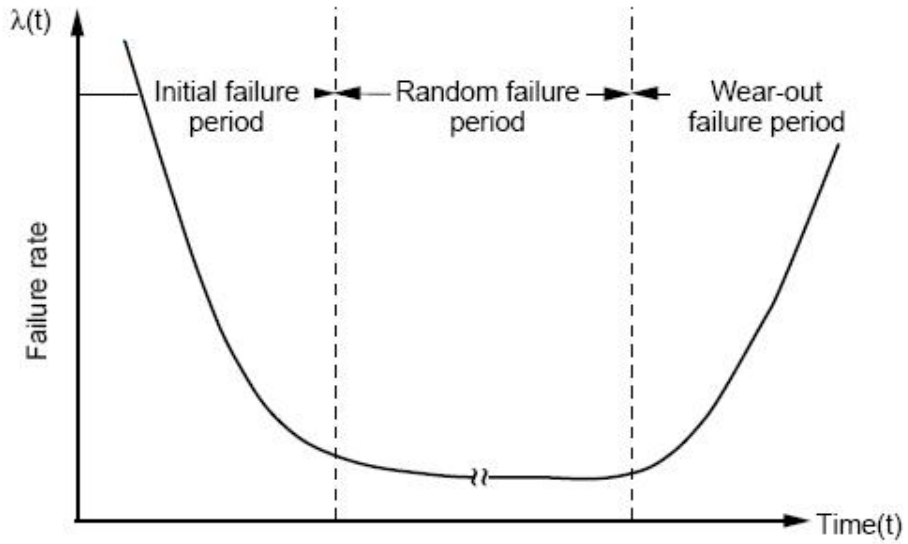
Commercial Network Availability

- **Commercial networks are typically built to an availability standard originally defined in Bellcore TR332. This standard is commonly referred to as "5 nines".**
- **Key design goal is maximizing network availability during busy hour in order to maximize revenue.**
  - Availability and Reliability are often used interchangeably, although not always accurately ☺
- **A common theme in public safety network discussions:**

"We need to be more reliable than commercial networks, they are built to 5 9's, so we need to be 6 9's."

Availability %	Downtime per year	Downtime per month*	Downtime per week
90%	36.5 days	72 hours	16.8 hours
95%	18.25 days	36 hours	8.4 hours
98%	7.30 days	14.4 hours	3.36 hours
99%	3.65 days	7.20 hours	1.68 hours
99.5%	1.83 days	3.60 hours	50.4 minutes
99.8%	17.52 hours	86.23 minutes	20.16 minutes
99.9% ("three nines")	8.76 hours	43.2 minutes	10.1 minutes
99.95%	4.38 hours	21.56 minutes	5.04 minutes
99.99% ("four nines")	52.6 minutes	4.32 minutes	1.01 minutes
99.999% ("five nines")	5.26 minutes	25.9 seconds	6.05 seconds
99.9999% ("six nines")	31.5 seconds	2.59 seconds	0.605 seconds

Failure Model



- **Although communications networks are generally repairable, it is not realistic to assume they can be repaired in a timely manner during an emergency, hence MTTF is the appropriate metric for public safety networks. MTTF = 1/ λ.**

- **The random failure period is where the public safety requirements diverge from commercial availability. The types of failures considered are assumed to be due to random, independent events, and this calculation does not provide any information on the failure rate due to a specific type of disaster event where failures are neither random or independent.**

Lessons from 9/11

Police Network was first to fail on 9/11

- The police network had two towers covering Manhattan, one of which was on the World Trade Tower. When the tower fell most of the local police network capacity was lost and any remaining communication channels were quickly flooded with so much traffic as to be rendered useless for emergency communication.

Cellular networks were the next to fail

- The commercial carriers have a far greater number of towers in Manhattan than the police network did, however loss of towers due to the collapse of the towers, resulting power failures in large parts of the city and extremely high call volume from private citizens and public safety officials trying to communicate brought effective communication to an halt.

Interestingly the one network that maintained some level of usability throughout the 9/11 crisis was WiFi

Source: 9/11 Commission Report

Why WiFi was Survivable ?

- **WiFi networks are not built to a 5 9's standard. The equipment is cheap and notoriously unreliable. The networks are connected through a variety of non-redundant backhaul methods including cable, DSL, microwave and conventional POTS lines. In addition, WiFi equipment is not typically designed with a battery backup system to withstand power failures.**

- **WiFi was survivable because of the large number of overlapping nodes, heterogeneously connected. Heterogeneity was a defense against the simultaneous, dependent failures that occur in disaster scenarios.**

- **One should *not* conclude from this example at WiFi is the solution for public safety communications. WiFi has many short comings in terms of range, building penetration, capacity and spectrum efficiency. The lesson from 9/11 communications is that heterogeneity in network design is critical to disaster survivability and that redundancy at the coverage level is essential. Building coverage redundancy with traditional equipment would be prohibitively expensive, but the WiFi example shows that low cost, non-5 9s, equipment can be used to cost effectively build a communications network that can provide survivable communications in disaster scenarios.**

Lessons from Katrina

- **FCC report on the Katrina aftermath identified the primary causes of communications infrastructure failures were power outages and failure of the backhaul networks connecting the cell sites to the networks**

Lessons from Katrina: Backhaul

- **The backhaul failures were primarily due to flooding and cable cuts in terrestrial or underground cables. Most of these failures did not occur during the storm, but in the flooding due to the levy breaks after the storm and many of the cable cuts actually happened during the repair of infrastructure after the storm and flooding.**

- **There were redundant core switches in different physical locations but the combination of flooding of one central office combined with fiber outages due to flooding which cut access to the secondary site brought down the landline network, and with it key public safety and commercial wireless capabilities. Even though the core switching was redundant, the multiple dependent failures brought the system down.**

- **The wireless networks run by the utility companies for their own communications were generally more robust. The primary reason for this was they were build with two backhaul connections, one terrestrial and one wireless, typically microwave. While the terrestrial component failed due to the flooding, the wireless connection fared much better.**

Lesson from Katrina: Power

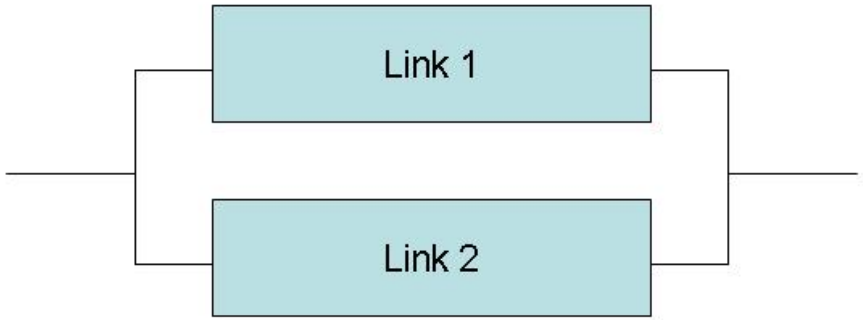
Power is a hard problem to tackle. the FCC report notes that even though many sites had diesel generators, the duration of the outage was longer than the fuel supply could sustain.

Replenishing the fuel supply was difficult because the was no access to the sites and in some cases file supplies were confiscated to support relief centers, hospitals and other priorities.

Unlike backhaul, we don't have redundant power networks to choose from

Implications for Public Safety Network Design

Backhaul Design: Redundant Heterogeneous Links



$$Ac = 1 - (1 - A)^2$$

- **One common approach to improving network availability is to introduce redundant parallel network paths, the availability of the combined system increases.**
- **However, in the case of a disaster, if both links are subject to the same failure mode, there is no increase in survivability.**
- **However, if the two links have different disaster failure modes, then we do in fact get the increase in overall link availability during a disaster. During Katrina some the wireless utility networks that employed this principle and deployed both T1 and microwave backhaul had a much better survival track cord.**
- **Furthermore, these paths can be lower cost than a single dedicated path, because each path can be a lower availability, lower cost, connection because the parallel combination of the two provides increased availability.**

Power Design

- **Heterogeneous redundancy into the power supply for communications site is not a feasible solution. As we have seen from the preceding examples the traditional approaches of batteries and diesel generators have significant limitations.**

- **Solution**
  1. Dramatically reduce the power consumption at each site. This would allow the backup battery or generator system to keep the site live for a longer period of time
  2. Use a large number of low power, low cost sites to achieve the coverage goal. Sites that cover a smaller area use dramatically less power. The power required to cover an areas is governed by a square law, so roughly speaking, to double the area covered, then power consumption of the site would have to be squared.

Network Architecture

A public safety network architecture consisting of a large number of low cost, smaller coverage area sites, will lead to a more survivable network, with better coverage, at lower cost.

- **More sites = Improved Survivability**
  - From a survivability point of view, more sites is better, as illustrated by the WiFI example during 9/11. Especially during event such as terrorist attacks that are more localized, a greater number of sites improves the possibility that some sites nearby are still available.
- **The traditional approach to dealing with site reliability is to throw money at the base station site to make it more robust to failure.**
  - Not only is this expensive, but there is no way to guarantee that nodes won't fail regardless of how much money is thrown at the problem.
- **There have been commercially successful examples of building very reliable systems from lower cost, less reliable components.**
  - RAID[1]disk arrays, the most common and cost effective method for reliable information storage, creates a reliable data storage system from redundant arrays of inexpensive disks, which is far more cost effective that building a single reliable storage system.
  - The same principle has been used to propose a cost effective, reliable approach to the exploration of Mars.[2] The approach put forth by Brooks and Flynn was to replace a single large 1000 kilogram rover by 100 smaller 1 kilogram rovers to explore planetary surfaces. The smaller robots could be built much cheaper and mass produced. They also offer redundancy in the case of occasional robot failure which in the case of a single larger robot would lead to total mission failure.
- **A larger number of low profile sites will also lead to improved coverage. When using traditional high sites, many factors including obstructions and multiple-path effects come into play to limit coverage. Multiple smaller sites can be located in and around buildings that might otherwise block coverage from high sites leading to more complete coverage in hard to cover areas such as urban canyons or inside of buildings.**

[1] Patterson, David; Garth A. Gibson, Randy Katz (1988). "A Case for Redundant Arrays of Inexpensive Disks (RAID)". *SIGMOD Conference*. pp. pp 109–116.
[2] Fast, cheap and out of control: A robot invasion of the solar system, Rodney Brooks and Anita M. Flynn, Journal of the British Interplanetary Society, Volume 42, pp 478-485, 1989.

Massive Disasters

- **The recent Tsunami in Japan make it clear that there are some situations where ground –based infrastructure cannot be relied on in the immediate aftermath of an emergency. During the first 72 hours of a response to such a disaster, communications may be partially or completely disrupted due to damaged facilities, widespread power outages, and lack of access by restoration crews and equipment to the impacted area. Non-terrestrial backup communications are the only viable option for providing communications in such scenarios.**

- **The operating principle in these scenarios must by that any communications is infinitely better than no communications. Even simple voice with no data is incredibly valuable in these situations.**

Summary: Design Principles for Survivable Public Safety Networks

- **Redundant, heterogeneous backhaul.**
  - *Survivability:* Heterogeneity is essential for survivability so that the two backhaul links are not susceptible to the same types of disaster failure modes.
  - *Cost Effectiveness:* This approach reduces the cost of backhaul as two parallel links have higher reliability than one single link, allowing each link to individually be lower reliability and lower cost, but achieving higher overall system reliability.

- **Minimize power consumption at each site.**
  - *Survivability:* In order to extend the life of sites during power failures, the power consumption at each site must be minimized to allow batteries or other alternative energy source to last as long as possible.
  - *Cost Effectiveness: Lower power consumption will lead to lower operating costs per site*

- **Large Number of low profile sites.**
  - *Survivability:* A large number of sites, deployed in an overlapping coverage scheme'
  - *Cost Effectiveness"* With a large number of lower profile sites economies of scale will lower cost of production. Furthermore, if deployed in a redundant overlapping configuration, each site can be built to a lower reliability tolerance individually, significantly reducing the cost of each site.